

1 This listing of claims will replace all prior versions, and listings, of claims
2 in the application:

3
4 **Listing of Claims**

5 Claim 1 (Currently amended): A session-state management method
6 comprising:

7 generating an encoded session-state token, wherein the token incorporates a
8 representation of session state of a client;

9 encrypting the encoded token using a one-way encryption scheme to
10 produce an encrypted token that cannot be decrypted; and

11 sending the encrypted token to the client.

12
13 Claim 2 (Original): A method as recited in claim 1, further comprising
14 authenticating the user of the client.

15
16 Claim 3 (Original): A method as recited in claim 1, further comprising
17 authenticating the user of the client, wherein the authenticating step comprises:

18 receiving a user identification indicator ("username") and a password;

19 comparing the username to a database of authorized user records, each
20 record containing a username and a username-associated password;

21 comparing the password received in the receiving step to a username-
22 associated password of a record containing a matching username; and

23 establishing a session for the user.

24 Claim 4 (Original): A method as recited in claim 1, wherein the generating
25 step comprises forming a confirmation token that incorporates a representation of
an incremental time block.

1 Claim 5 (Original): A method as recited in claim 1, wherein the generating
2 step comprises forming a confirmation token that incorporates a representation of a
3 current incremental time block.
4

5 Claim 6 (Original): A method as recited in claim 1, wherein the generating
6 step comprises forming a confirmation token that incorporates a representation of
7 an incremental time block that is prior a current incremental time block.
8

9 Claim 7 (Original): A computer-readable storage medium having
10 computer-executable instructions that, when executed by a computer, performs the
11 method as recited in claim 1.

12 Claim 8 (Currently amended): A session-state management method
13 comprising:
14

15 receiving an one-way encrypted, session-state token that cannot be
16 decrypted from a client, wherein the token incorporates a representation of session
17 state of a client;

18 generating an one-way encrypted, confirmation session-state token that
19 cannot be decrypted; and
20

21 comparing the confirmation token with the received token.
22

23 Claim 9 (Original): A method as recited in claim 8, wherein the generating
24 step comprises forming a confirmation token that incorporates a representation of
25 an incremental time block.

Claim 10 (Original): A method as recited in claim 8, wherein the
generating step comprises forming a confirmation token that incorporates a

1 representation of a current incremental time block.

2 Claim 11 (Original): A method as recited in claim 8, wherein the
3 generating step comprises forming a confirmation token that incorporates a
4 representation of an incremental time block that is prior a current incremental time
5 block.

6
7 Claim 12 (Currently amended): A method as recited in claim 8, further
8 comprising:

9 issuing an ~~one-way~~ encrypted, replacement session-state token that cannot
10 be decrypted; and

11 sending the replacement token to the client.

12 Claim 13 (Original): A method as recited in claim 12, wherein the issuing
13 step comprises forming a replacement token that incorporates a representation of a
14 current incremental time block.

15
16 Claim 14 (Currently amended): A method as recited in claim 8, wherein the
17 generating step comprises forming a confirmation token that incorporates a
18 representation of an incremental time block, if confirmation and received tokens
19 fail to match, the method further comprising:

20 generating a new ~~one-way~~ encrypted, confirmation session-state token that
21 cannot be decrypted, wherein the confirmation token incorporates a representation
22 of a previous incremental time block; and

23 comparing the new confirmation token with the received token.
24
25

1 Claim 15 (Currently amended): A session-state management method
 2 comprising:

3 receiving a one-way encrypted session-state token from a client, wherein
 4 the token incorporates a representation of session state of a client;

5 generating a one-way encrypted confirmation session-state token; and

6 comparing the confirmation token with the received token;

7 wherein the generating step comprises forming a confirmation token that
 8 incorporates a representation of an incremental time block, if confirmation and
 9 received tokens fail to match;

10 generating a new one-way encrypted confirmation session-state token,
 11 wherein the confirmation token incorporates a representation of a previous
 12 incremental time block; and

13 comparing the new confirmation token with the received token;

14 ~~A method as recited in claim 14, wherein the new-confirmation-token~~
 15 ~~generating step comprises forming a confirmation token that incorporates a~~
 16 ~~representation of an incremental time block, if confirmation and received tokens~~
 17 ~~fail to match, the method further comprising: and~~

18 repeating the steps of new-confirmation-token generating and comparing
 19 the new and received tokens, wherein each subsequent reiteration of such steps
 20 employs a representation of a previous incremental time block that is previous a
 21 previous reiteration of the same steps, for a specified number of times or until
 22 compared tokens match.
 23
 24
 25

1 Claim 16 (Original): A computer-readable storage medium having
2 computer-executable instructions that, when executed by a computer, performs the
3 method as recited in claim 8.

4
5 Claim 17 (Original): A session-state management method comprising:

6 (A) receiving a one-way encrypted, session-state token from a client;

7 (B) generating a one-way encrypted, confirmation session-state token,
8 wherein the confirmation token incorporates a representation of a current
9 incremental time block;

10 (C) comparing the confirmation token with the received token;

11 (D) if the confirmation token and the received token match,

12 (1) issuing a one-way encrypted, replacement session-state token, wherein
13 the replacement token incorporates a representation of a current incremental time
14 block;

15 (2) sending the replacement token to the client.

16 if the confirmation token and the received token fail to match,

17 (3) generating a new one-way encrypted, confirmation session-state token
18 using the one-way encryption scheme of the encryption step, wherein the token
19 incorporates a representation of a previous incremental time block;

20 (4) comparing the new confirmation token with the received token;

21 (5) if the new confirmation and received tokens fail to match, then further
22 comprising:

23 (i) repeating the steps of new-confirmation-token generating and comparing
24 the new and received tokens, wherein each subsequent reiteration of such steps
25 employs a representation of a previous incremental time block that is previous a
previous reiteration of the same steps, for a specified number of times;

(ii) if, during the repeating step, the confirmation token matches the

received token,

(a) issuing a one-way encrypted, replacement session-state token, wherein the token incorporates a representation of a current incremental time block;

(b) sending the replacement token to the client.

Claim 18 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 17.

Claim 19 (Original): A session-state management method comprising:
authenticating a user of a client to establish a session with the user;
generating an encoded session-state token, wherein the encoded token incorporates a representation of session-state of the user's session;
encrypting the encoded token to produce an encrypted token that cannot be decrypted; and
sending the encrypted session-state token to the client.

Claim 20 (Original): A method as recited in claim 19, wherein the authenticating step comprises:
receiving a user identification indicator ("username") and a password;
comparing the username to a database of authorized user records, each record containing a username and a username-associated password;
comparing the password received in the receiving step to a username-associated password of a record containing a matching username; and
establishing a session for the user.

1 Claim 21 (Original): A method as recited in claim 19, wherein:
2 the user is identified by a user identification indicator (UserID);
3 the generating step comprises forming a session-state token at least partially
4 based upon the UserID.

5 Claim 22 (Original): A method as recited in claim 19, wherein:
6 a time block is identified by a time block identification indicator (TimeID);
7 the generating step comprises forming a session-state token at least partially
8 based upon the TimeID.

9
10 Claim 23 (Original): A method as recited in claim 19, wherein:
11 the user is identified by a user identification indicator (UserID);
12 a time block is identified by a time block identification indicator (TimeID);
13 the generating step comprises forming a session-state token at least partially
14 based upon the UserID and the TimeID.

15 Claim 24-25 (Canceled)

16
17 Claim 26 (Original): A method as recited in claim 19, wherein:
18 the user is identified by a user identification indicator (UserID);
19 a time block is identified by a time block identification indicator (TimeID);
20 the generating step comprises combining UserID and TimeID to produce an
21 encoded token.

22 Claim 27 (Original): A computer-readable storage medium having
23 computer-executable instructions that, when executed by a computer, performs the
24 method as recited in claim 19.
25

1 Claim 28 (Currently amended): A session-state token generation method,
2 wherein an authenticated user is identified by a user identification indicator
3 (UserID) and a time block identification indicator (TimeID) identifies a specific
4 time block, the method comprising:

5 combining UserID and TimeID to produce an encoded token;

6 encrypting the encoded token to produce an encrypted token that cannot be
7 decrypted.

8 Claim 29 (Original): A method as recited in claim 28, wherein the
9 combining step comprises concatenating UserID and TimeID.

10 Claim 30 (Original): A method as recited in claim 28, wherein the
11 combining step comprises concatenating UserID, TimeID, and a code key.

12
13 Claim 31 (Original): A method as recited in claim 28, wherein the
14 encrypting steps comprises encrypting the encoded token using a one-way
15 encryption scheme.

16 Claim 32 (Original): A method as recited in claim 28, wherein the
17 encrypting steps comprises:

18 encrypting the encoded token using a one-way encryption scheme to
19 produce an encrypted result; and

20 selecting a defined portion of the encrypted result to form a session-state
21 token.

22
23 Claim 33 (Original): A computer-readable storage medium having
24 computer-executable instructions that, when executed by a computer, performs the
25 method as recited in claim 28.

1 Claim 34 (Currently amended): A session-state management method
2 comprising:

3 receiving a user-associated, encoded session-state token that cannot be
4 decrypted from a client, wherein the encoded token incorporates a representation
5 of session-state of the user's session;

6 generating an encoded, confirmation session-state token;

7 encrypting the encoded confirmation token to produce an encrypted token
8 that cannot be decrypted; and

9 comparing the received token with the confirmation token.

10 Claim 35 (Original): A method as recited in claim 34, wherein the
11 generating step comprises forming a confirmation token that incorporates a
12 representation of a current incremental time block, if confirmation and received
13 tokens fail to match, further comprising:

14 generating a new confirmation token using a representation of a incremental
15 time block previous of the time block representation used for the previous
16 generating step;

17 comparing the new confirmation token with the received token.

18 Claim 36 (Currently amended): A session-state management method
19 comprising:

20 receiving a user-associated, encoded session-state token from a client,
21 wherein the encoded token incorporates a representation of session-state of the
22 user's session;

23 generating an encoded, confirmation session-state token;

24 comparing the received token with the confirmation token;

25 wherein the generating step comprises forming a confirmation token that

1 incorporates a representation of a current incremental time block, if confirmation
2 and received tokens fail to match, further comprising:

3 generating a new confirmation token using a representation of a incremental
4 time block previous of the time block representation used for the previous
5 generating step;

6 comparing the new confirmation token with the received token; and

7 ~~A method as recited in claim 35, if confirmation and received tokens fail to~~
8 ~~match, further comprising; and~~

9 repeating the steps of generating a new confirmation token and comparing
10 the new and received tokens, wherein each subsequent reiteration of these steps
11 uses a representation of a previous incremental time block that is previous—a
12 previous reiteration of the same steps, for a specified number of times or until
13 compared tokens match.

14
15 Claim 37-38 (Canceled)

16 Claim 39 (Original): A computer-readable storage medium having
17 computer-executable instructions that, when executed by a computer, performs the
18 method as recited in claim 34.

19 Claim 40 (Currently amended): A session-state management method
20 comprising:

21 receiving an encoded token that cannot be decrypted comprising a user-
22 associated TimeID from a client, wherein the encoded token incorporates a
23 representation of session-state of the user's session;

24 designating a first time block identification indicator (TimeID) for a first
25 time block; and

comparing the user-associated TimeID with the first TimeID.

1 Claim 41 (Currently amended): The method of claim 40, further
2 comprising:

3 designating a prior TimeID for a time block prior to the first time block; and
4 comparing the user-associated TimeID with the prior TimeID.

5
6 Claim 42 (Currently amended): A server to communicate with a client over
7 a communications network, the server comprising:

8 a processor; and

9 a session-state manager executable on the processor to:

10 generate a session-state token, wherein the token incorporates a
11 representation of session state of the client;

12 encrypt the token using ~~a one-way encryption scheme~~ to produce an
13 encrypted token that cannot be decrypted; and

14 send the encrypted token to the client.

15 Claim 43 (Currently amended): A server to communicate with a client over
16 a communications network, the server comprising:

17 a processor; and

18 a session-state manager executable on the processor to:

19 receive an one-way encrypted, session-state token that cannot be decrypted
20 from the client, wherein the token incorporates a representation of session state of
21 a client;

22 generate an one-way encrypted, confirmation session-state token that cannot
23 be decrypted; and

24 compare the confirmation token and the received token.
25

1 Claim 44 (Currently amended): A server to communicate with a client over
2 a communications network, the server comprising:

3 a processor; and

4 a session-state manager executable on the processor to:

5 authenticate a user of the client;

6 generate an encoded session-state token, wherein the token incorporates a
7 representation of session state of the client; and

8 encrypt the session-state token into a token that cannot be decrypted; and

9 send the encrypted session-state token to the client.

10 Claim 45-46 (Canceled)

11 Claim 47 (Currently amended): A server to communicate with a client over
12 a communications network, wherein an authenticated user is identified by a user
13 identification indicator (UserID) and a time block identification indicator
14 (TimeID) identifies a specific time block, the server comprising:

15 a processor; and

16 a session-state manager executable on the processor to:

17 combine UserID and TimeID to produce an encoded token; and

18 encrypt the encoded token into a token that cannot be decrypted.

19 Claim 48 (Currently amended): A server to communicate with a client over
20 a communications network, the server comprising:

21 a processor; and

22 a session-state manager executable on the processor to:

23 receive a user-associated, encoded session-state token from the client;

24 generate an encoded, confirmation session-state token, wherein the
25 confirmation token incorporates a representation of session state of the client;

1 encrypt the encoded token into a token that cannot be decrypted; and
2 compare the received token with the confirmation token.

3 Claim 49 (Currently amended): A computer-readable storage medium
4 having computer-executable instructions that, when executed by a computer,
5 performs the method comprising:

6 generating an encoded session-state token, wherein the token incorporates a
7 representation of session state of a client;

8 encrypting the encoded token into a token that cannot be decrypted using a
9 one-way encryption scheme; and

10 sending the encrypted token to the client.

11 Claim 50 (Currently amended): A computer-readable storage medium
12 having computer-executable instructions that, when executed by a computer,
13 performs the method comprising:

14 receiving an one-way encrypted, session-state token that cannot be
15 decrypted from a client, wherein the token incorporates a representation of session
16 state of a client;

17 generating an one-way encrypted, confirmation session-state token that
18 cannot be decrypted; and

19 comparing the confirmation token with the received token.